Incident Reporting Form

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | | | | |
| **I am:**  the effected entity ☑ reporting incident affecting other entity | | | | |
| **Contact Information of the Reporter** | | | | |
| Name & Role/Title |  Individual ☑ Organization | | | |
| Organization name (if any) | CatchPhish | | | |
| Contact No. | 8779959071 | | Email: | catchphish@gmail.com |
| Address: | Kj Somaiya college of engineering | | | |
| **Basic Incident Details** | | | | |
| Affected entity  (if not same as reporting entity above) | | Union bank of India | | |
| Incident Type | | | | |
| Targeted scanning/probing of critical  Data Breach Attacks or malicious/suspicious activities  networks/systems  Data Leak affecting systems/ servers/ networks/  Compromise of critical systems/information Attacks on Internet of Things (IoT) devices software/ applications related to Big Data,  Unauthorised access of IT systems/data and associated systems, networks Block chain, virtual assets, virtual asset  Defacement or intrusion into the website software, servers exchanges, custodian wallets, Robotics, 3D  Malicious code attacks Attacks or incident affecting Digital and 4D Printing, additive manufacturing,  Attack on servers such as Database, Mail and DNS Payment systems Drones  and network devices such as Routers Attacks through Malicious mobile Apps Attacks or malicious/ suspicious activities  ☑Identity Theft, spoofing and phishing attacks Fake mobile Apps affecting systems/ servers/software/   DoS/DDoS attacks  Unauthorised access to social media applications related to Artificial Intelligence  Attacks on Critical infrastructure, SCADA and accounts and Machine Learning operational technology systems and Wireless Attacks or malicious/ suspicious activities  Other (Please Specify)  networks affecting Cloud computing ----------------------------------------------------------  Attacks on Application such as E-Governance, E- systems/servers/software/applications  Commerce etc. ---------------------------------------------------------- | | | | |
| Is the affected system/network critical to the organization’s mission? (Yes / No). (Brief details.) | | Yes | | |
| Basic Information of Affected System (Provide information that is readily available.) | | Domain/URL: http://www.onlinesbi.sbi IP Address: 103.68.221.190 Operating System:Unknown (Hosting Server Details Not Available) Make/ Model/Cloud details: Hosted by Unknown Affected Application details (If any): Potential phishing website at www.onlinesbi.sbi Location of affected system (including City, Region & Country): Unknown  Network and name of ISP: Unknown, IP: 103.68.221.190 | | |
| Brief description of Incident: A potential phishing website was detected at www.onlinesbi.sbi. Risk Score: 28.57/10 (Confidence: Low). The site was created on 27/04/2020 13:00 UTC.   Risk Analysis: - Login form legitimacy: The login forms link to official SBI domains (retail.onlinesbi.sbi, yonobusiness.sbi, corp.onlinesbi.sbi), reducing the risk of phishing on this landing page. However, users must always verify the URL. - Brand impersonation: The site appears to use official SBI branding, which reduces the risk of brand impersonation \*on this landing page\*. This doesn't guarantee the legitimacy of \*linked\* pages. - Malicious JavaScript: The presence of obfuscated JavaScript (starting with `var resizea=['0\x27/>', ... ]`) raises suspicion. Obfuscation is often used to hide malicious code. The `f5\_cspm` script is likely related to F5 security products and is less likely to be malicious, but it's still important to audit its behavior if this were a real-world scenario. - Social engineering: The disclaimer "SBI never asks for confidential information such as PIN and OTP from customers..." is a good sign, indicating awareness of social engineering risks. However, the page itself might be a \*precursor\* to a social engineering attack if users are directed to a fake login page after clicking a link. - Reliance on External Links: The website heavily relies on external links (<a> tags with href attributes) to various banking services, forms, and other resources. While many of these links appear legitimate, the security of the \*overall user experience\* depends heavily on the security and integrity of these external domains. A compromised external site could be exploited to conduct phishing attacks or distribute malware. - Use of Javascript `window.open`: The use of Javascript's `window.open` function presents a risk, as the linked page might be crafted to look similar to the legitimate one to phish credentials or other information. - New User Registration Modal: The 'New User Registration' modal could be a target for phishing attempts, gathering user information under the guise of registration.  The domain is registered with Unknown. VirusTotal scan shows 0 engines flagged this domain as malicious out of 94 total engines. Immediate intervention is recommended to prevent potential data theft and financial fraud. | | Occurrence date & time (dd/mm/yyyy hh:mm): 27/04/2020 13:00 UTC Detection date & time (dd/mm/yyyy hh:mm): 18/03/2025 10:09 UTC | | |
| **Note:** (i) This form provides general guidance in terms of information which could be relevant to the incident.   1. It is not mandatory to fill and/or sign this form. Incidents may also be reported by providing relevant information in the communication itself or in any other readable form. 2. Reporting entity may, if desired, also provide relevant information other than mentioned in this form. | | | | |
| **Mail/Fax incident reports to: CERT-In, Electronics Niketan, CGO Complex, New Delhi 110003 Fax:+91-11-24368546 or email at:** [**incide**](mailto:incident@cert-in.org.in)[**nt@cert-in.org.in**](mailto:nt@cert-in.org.in) | | | | |